NATIONAL SECURITY AGENCY
INFORMATION ASSURANCE DIRECTORATE

Commercial Solutions for Classified (CSfC)
Data-at-Rest (DAR)
Capability Package

Version 0.8
03 July 2014

CHANGE HISTORY

Title	Version	Date	Change Description
Commercial Solutions for Classified (CSfC) Data at Rest (DAR) Capability Package	0.8		• Initial draft of CSfC Data at Rest (DAR) guidance.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

1. INTRODUCTION

The Commercial Solutions for Classified (CSfC) program within the National Security Agency (NSA) Information Assurance Directorate (IAD) uses a series of Capability Packages (CP) to provide configurations that will allow customers to independently implement secure solutions using layered Commercial Off-the-Shelf (COTS) products. The CP is vendor-agnostic and provides high-level security and configuration guidance for customers and/or Solution Integrators.

The IAD within the NSA is delivering a generic CSfC Data-at-Rest (DAR) CP to meet the demand for data at rest solutions using a Secure Sharing Suite (S3) of algorithms (NSA Suite B algorithms). These algorithms are used to protect classified data using layers of COTS products. DAR CP Version 0.8 enables customers to implement two independent layers of encryption for the purpose of providing protection for stored information while the End User Device (EUD) is unpowered or in an unauthenticated state. This CP takes lessons learned from one proof-of-concept demonstration per solution design that has implemented a set of S3 algorithms, modes of operation, standards, and protocols. These demonstrations included a layered use of COTS products for the protection of classified information.

2. PURPOSE OF THIS DOCUMENT

This CP provides high-level reference designs and corresponding configuration information allowing customers to select COTS products from the CSfC Components List, available on the CSfC web page (http://www.nsa.gov/ia/programs/csfc_program) for their DAR solution and then properly configure those products to achieve a level of assurance sufficient for protecting classified data while at rest. As described in Section 9, customers must ensure the components selected from the CSfC Components List will permit the necessary functionality for the selected capabilities. Throughout this document, requirements imposed on the DAR solution to ensure proper implementation are identified by a label consisting of the prefix "DAR," a two-letter category, and a sequence number (e.g., DAR-KM-2). To successfully implement a solution based on this CP, all Threshold requirements, or the corresponding Objective requirements, applicable to the selected capabilities must be implemented, as described in Section 8. Customers who want to use a variant of the solution detailed in this CP must contact NSA to determine ways to obtain NSA approval. Additional information about the CSfC process is available on the CSfC web page (www.nsa.gov/ia/programs/csfc_program).

3. USE OF THIS DOCUMENT

This is draft Version 0.8 of the DAR CP dated May 2014, for community review. Please provide comments on usability, applicability, and/or shortcomings to your NSA/IAD Client Advocate and the DAR CP maintenance team at dl_csfc_dar_team@nsa.gov.

The following Legal Disclaimer relates to the use of this CP:

This CP is provided “as is.” Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data, or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this CP, even if advised of the possibility of such damage.

The User of this CP agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorney’s fees, court costs, and expenses, arising in direct consequence of recipient’s use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this CP is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer’s product or service.

4. DAR PROTECTION OVERVIEW

The goal for the DAR solution is to protect classified data when the EUD is powered off or unauthenticated. Specific data to be protected must be determined by the data owner. An EUD is the computing device where the DAR solution is hosted.

As the portability of EUDs increases, the requirements for when and how classified data is protected also increases. EUDs can be used in both physically protected and physically unprotected environments. Solutions using commercial products must protect classified data on the EUD by using two layers of encryption with approved Suite B algorithms listed in Table 1: Approved Suite B DAR Algorithms. This CP provides two solution designs for DAR protection. Each solution design has specific requirements for configuration, product selection, components, provisioning, authentication, key management, operations, administration, roles, use and handling.

Table 1: Approved Suite B DAR Algorithms

Security Service	Algorithm Suite 1	Algorithm Suite 2	Specifications
Overall Level of Security	128 bits	192 bits	
Confidentiality (Encryption)	AES-128	AES-256	FIPS PUB 197 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Authentication (Digital Signature)	ECDSA over the curve P-256 with SHA-256	ECDSA over the curve P-384 with SHA-384	FIPS PUB 186-3 IETF RFC 6239 IETF RFC 6380 IETF RFC 6460
	RSA 2048 (prior to 1 October 2015)	N/A	FIPS PUB 186-3
	DSA 2048 (prior to 1 October 2015)	N/A	FIPS PUB 186-3
Integrity (Hashing)	SHA-256	SHA-384	FIPS PUB 180-4 IETF RFC 6239 IETF RFC 6379 IETF RFC 6380 IETF RFC 6460
Can protect	Up to Secret	Up to Top Secret	

The two solution designs in this CP are limited to addressing the mechanisms used to provide DAR protection. This CP is focused on the implementation of cryptography to mitigate the risk to classified data from unauthorized access when the device is powered off or unauthenticated. This CP does not protect against the possibility of malicious code exploits, updates, Operating System (OS) misconfigurations, or the persistence of remnants of key or plaintext material in volatile memory on the EUD when powered-on.

Although the DAR solution designs can protect the confidentiality of data and render the EUD unclassified, it does not protect the integrity of an EUD outside of the control of approved users. It is difficult to examine and determine whether or not a device has been tampered with. Therefore, the NSA requires implementing organizations to define the cirumstances in which an EUD that is part of the organization's solution to be considered outside of the positivie control of authorized users (i.e., "lost"). Organizations must also define the cirumstances in which an EUD that is a part of that organization's solution is to be considered recovered back into the positive control of authorized users (i.e., "found"). This CP requires any lost device, once found to be destroyed in order to mitigate threats to the integrity of the EUD and any connected systems. This requirement to destroy "found" EUDs does not preclude an implementing organization from first performing a forensic examination on a "found" device to discover better ways to protect the organization's EUDs.

4.1 RATIONALE FOR LAYERED ENCRYPTION

A single layer of Suite B encryption, properly implemented, is sufficient to protect classified data at rest. The DAR solution uses two layers of Suite B encryption not because of a deficiency in the cryptographic algorithms, but rather to mitigate the risk that a failure in one of the DAR components, whether by accidental misconfiguration, operator error, or malicious exploitation of an implementation vulnerability, results in exposure of classified information. The use of multiple layers, implemented with components meeting the CSfC vendor diversity requirements reduces the likelihood a single vulnerability can be exploited to reveal protected information.

If one of the DAR layers is compromised or fails in some way, the second DAR layer can still provide the needed encryption to safeguard the classified data. If both layers are compromised or fail simultaneously, it is possible the classified data will become readable to a threat actor. The security of the DAR solution depends on preventing this failure mode by configuring a solution with two layers. The goal is to configure the solution in which both layers will not fail at the same time.

4.2 RED, GRAY, AND BLACK DATA

This CP uses the following terminology to describe the data types that comprise a DAR solution. The terms Red, Gray, and Black identify the number of encryption layers applied to classified data for a specific EUD state.

Red data is unencrypted classified data being processed by the EUD. After a user successfully authenticates to the outer and inner layers of DAR encryption, the EUD is in a state of processing Red Data.

Gray data contains classified information that has been encrypted once. After a user successfully authenticates to the outer layer of DAR encryption, but has not yet authenticated to the inner layer of encryption, the EUD is in a state of processing Gray Data.

Black data contains classified information that has been encrypted twice. An EUD is considered black when the device is powered off and/or unauthenticated and the stored data is encrypted with both the outer and inner layers.

5. SOLUTION COMPONENTS

5.1 SOFTWARE FULL DISK ENCRYPTION

Software Full Disk Encryption (SWFDE) is approved to provide the outer layer of DAR protection. All data on the hard drive used to boot the computer, including the computer's OS, is transparently encrypted by the Data Encryption Key (DEK), while permitting access to the data only after successful authentication to the SWFDE product and the Pre-Boot Environment (PBE). In the case of the SWFDE, the system hardware provides the resources to perform the encryption. This DEK is masked using a Key Encryption Key (KEK), and proper user authentication is required to decrypt the contents of the disk.

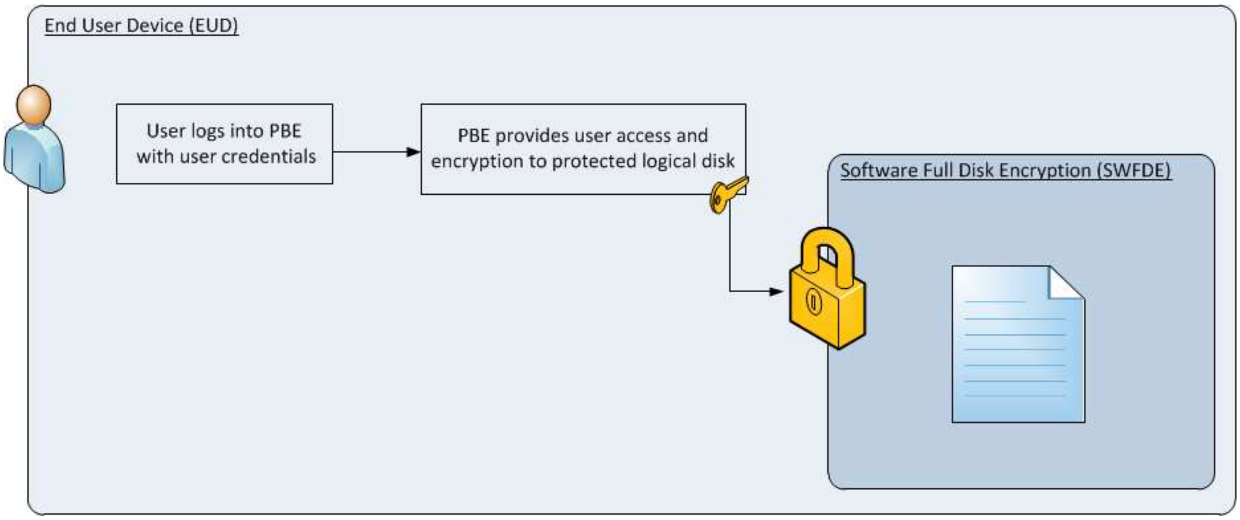
End User Device (EUD)
User logs into PBE with user credentials
PBE provides user access and encryption to protected logical disk
Software Full Disk Encryption (SWFDE)

Figure 1: Software Full Disk Encryption

5.2 PLATFORM ENCRYPTION

Platform Encryption (PE) is also approved to provide the outer layer of DAR protection. PE is provided by the operating system (e.g. Kernel) for platform-wide data encryption. The PE layer requires hardware-backed secure key storage and entropy collection. There are two major types of keys: DEKs and KEKs. A Root Encryption Key (REK) is considered a KEK. DEKs are used to encrypt data, and KEKs are used to encrypt other keys, such as DEKs and other KEKs. The DEK is masked using a REK or KEK. All data on the EUD, including the EUD OS, is encrypted by the DEK, while permitting access to the data only after successful authentication to the PE layer.

The basis of trust on the platform is hardware. A hardware-backed noise source is used for entropy generation. When mixed with a noise source, random numbers generated by the hardware perform two functions: they provide for the outer layer of encrypted data and they increase the assurance that authorization factors are properly chained back to trusted hardware.

With the exception of the hardware-specific requirements, there is little distinction between PE and File Encryption (FE) implementations, which are described in the following section, Section 5.3. In all other respects, the two component implementations are virtually identical; they both provide volume and file encryption capabilities.

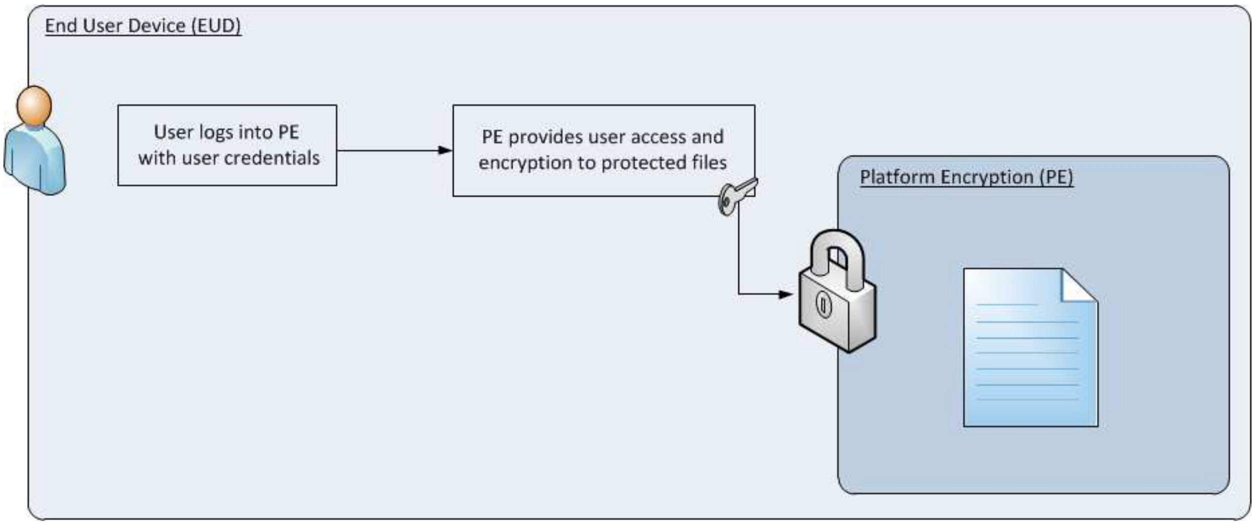
End User Device (EUD)
User logs into PE with user credentials
PE provides user access and encryption to protected files
Platform Encryption (PE)

Figure 2: Platform Encryption

5.3 File Encryption

File Encryption is approved to provide the inner layer of DAR protection. In this CP, the FE layer does not require hardware-backed secure key storage and entropy collection. File encryption products currently on the market have a wide range of implementations ranging from selecting individual files to whitelisting all but a few files. It is important for the user and implementer to understand how a specific file encryption product operates to ensure they encrypt all classified data on the EUD. There are many events and applications that may write data to the disk. Users should be made aware of these unless the FE product can encrypt the data without their intervention.

Each application handling classified data should be evaluated to ensure any such files it creates or modifies are either included in the encryption or do not include classified data. Examples include:

1. Temporary files that may contain data.
2. Paging files (i.e., swap files) are created when the system runs out of or becomes low on unused volatile memory (RAM). When this occurs, the system will write to the hard disk for storage. If the product can not automatically protect this data, the solution should disable system page files.
3. System restore and other features that allow data to be restored to a previous point in time create copies of the data. If this is enabled it may allow an encrypted file to be restored to

a state before it was encrypted. Unless the product accounts for these types of scenarios, such features should be disabled.

4. Memory dump files may be created when an error occurs. These dump files may include classified data that existed in volatile memory when the crash occurred. Since these files are created during a system crash, it is likely the product will not be able to properly encrypt them. Therefore, it is recommended this feature be disabled.
5. Printer spool files are created when a document is sent to print. These are used to hold the document while it is in queue for printing. If the solution is going to print any classified information these files should be protected.
6. Moving or deleting files: Users should be informed that moving (cut/paste) a classified file into a protected area is not sufficient for protecting it. Moving or deleting a file while it is unencrypted may leave file contents on the disk until it is overwritten by the file system. All files should be encrypted before being deleted or moved. When and where a file is encrypted may vary greatly between products.

The FE protects the confidentiality of individual files, folders, or volumes, and may be accomplished in several ways. The encryption may be performed by the application, platform, or the host OS. Each encrypted file or volume will be protected by a File Encryption Key (FEK). The FEK is protected by the user's credentials, either directly or through one or more KEKs.

Proper user authentication is required to decrypt the FEK. The FE product will then transparently decrypt files or directories on an individual basis as they are requested by the user via specific applications. To ensure no classified data is left unprotected, the Authorizing Official (AO)/ Designated Approving Authority (DAA) shall be responsible for providing and enforcing a policy which mandates automation and user compliance to encrypt all classified data.

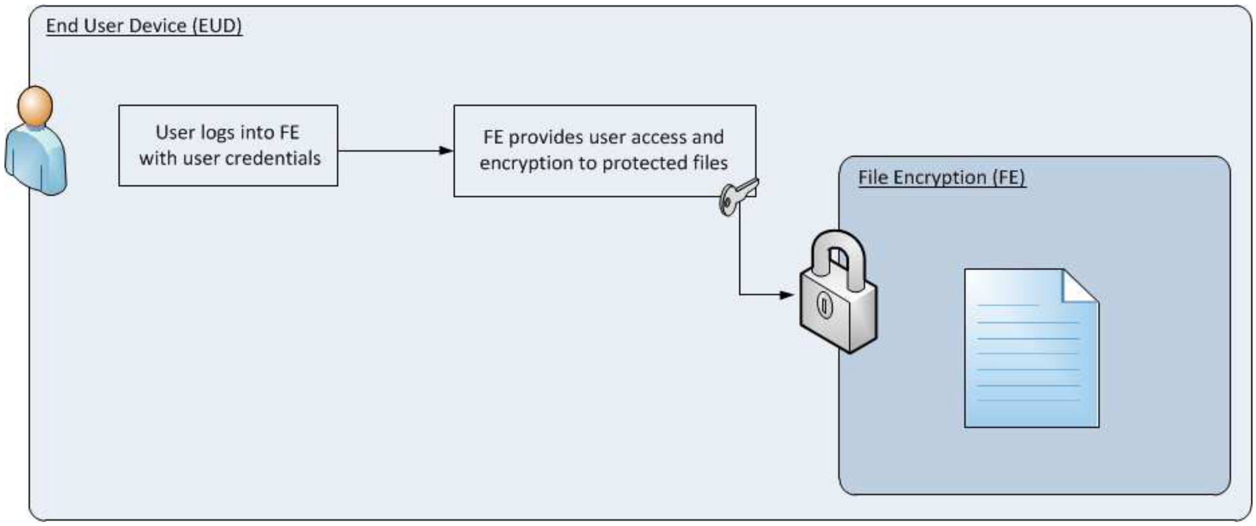
End User Device (EUD)
User logs into FE with user credentials
FE provides user access and encryption to protected files
File Encryption (FE)

Figure 3: File Encryption

5.4 END USER DEVICE

The End User Device is a commercial tablet, laptop, workstation, smart phone, or similar computing device that directly interacts with the DAR components. An EUD can operate within a secure physical environment approved by the AO/DAA or used outside of a secure physical environment.

5.4.1 PROVISIONING

Provisioning is the process through which EUDs are initialized before first use. During the provisioning process, the Security Administrator loads and configures the DAR components for the EUD. Provisioning is inherently an out-of-band process requiring physical access to the EUD.

This CP allows for EUD re-provisioning or re-use of DAR components as long as it is performed in accordance with this CP. If reprovisioning, the unencrypted data secured on the device must be at the same classification level of the previous unencrypted data stored on the approved DAR solution. Re-provisioning EUD components from any other solution design or non-CSfC solution is prohibited.

6. SOLUTION DESIGNS

The CP provides two solution designs. These designs describe solutions meeting a wide variety of requirements to protect classified DAR. In all cases, the customer will decide which design to pursue for registration in accordance with the DAR CP.

The first design covered is composed of SWFDE and FE. This design is designated “SF”. The second design covered is composed of PE and FE. This design is designated “PF”. The SF architecture is typically intended for EUDs such as servers, desktops, most laptops, and most tablets, while the PF solution design is intended for most cellular EUDs, including laptops, tablets, and smartphones.

Solution Design	Designator	Description
SWFDE / FE	SF	DAR solution architecture that layers FE on top of SWFDE, as described in Sections 6.1. Typically intended for servers, desktops, some laptops, and some tablets.
PE / FE	PF	DAR solution architecture that layers FE on top of PE, as described in Sections 6.2. Typically intended for some laptops, some tablets, and smartphones.

Table 2: Solution Design Summary

In both solution designs, the solution is contained in an individual EUD. Regardless of which architecture a DAR solution falls under, the implementation must meet all threshold requirements in the appropriate solution design section.

6.1 SWFDE/FE (SF) SOLUTION DESIGN

The SF Solution Design approach permits full disk/file/directory/volume encryption/decryption. In the SF solution design, DAR provided by the SWFDE will be used as the outer layer and FE provided by an application or OS will be used to provide the inner layer. The SF DAR solution uses a password, smart card, or Universal Serial Bus (USB) token to provide access to classified data. Once a user inputs the correct password, smart card, or USB token, the system boots the operating system. Next, the user authenticates to the FE which in turn decrypts the user's classified file. The SF solution is depicted below in Figure 4: SF Solution Design.

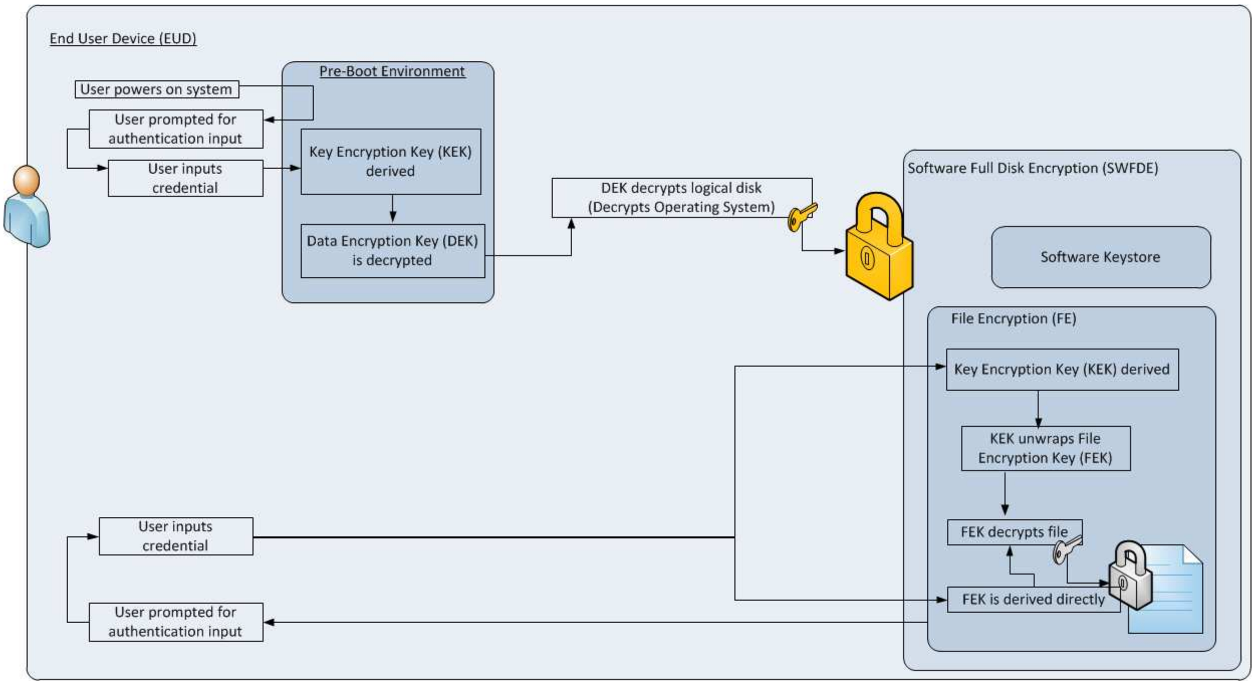
End User Device (EUD)
Pre-Boot Environment
User powers on system
User prompted for authentication input
User inputs credential
Key Encryption Key (KEK) derived
Data Encryption Key (DEK) is decrypted
DEK decrypts logical disk (Decrypts Operating System)
Software Full Disk Encryption (SWFDE)
Software Keystore
File Encryption (FE)
Key Encryption Key (KEK) derived
KEK unwraps File Encryption Key (FEK)
FEK decrypts file
FEK is derived directly
User inputs credential
User prompted for authentication input

Figure 4: SF Solution Design

Each layer of encryption in the SF DAR solution may use similar authentication mechanism types (e.g., passwords, tokens) but requires a unique authentication credential for each layer. For the first layer of encryption the user will authenticate to the PBE provided by the SWFDE. For the second layer the user will use their OS login credentials, application credentials, or file-specific credentials to authenticate to the FE.

6.1.1 SF SOLUTION STATES

Powered Off State:

In a powered off state, the device is completely off and not in any power saving state. The EUD is considered Unclassified but must still be handled in accordance with the implementing organization’s AO/DAA policies.

Powered On and Unauthenticated State:

In a powered on and unauthenticated state, the EUD is completely on, but the user has not logged in to either layer. The EUD is considered Unclassified, but must be handled in accordance with the implementing organization’s AO/DAA policies.

Powered On with Outer Layer Authenticated State:

In a powered on with Outer layer authenticated state, the device is operational where the user has authenticated to the outer layer of encryption. The device is considered classified and should be handled accordingly.

Powered On with Outer and Inner Layer Authenticated State:

In a powered on with outer and inner layers authenticated state, the EUD is operational, where the user has authenticated to two layers of DAR encryption. The device is considered classified and should be handled accordingly.

Locked State:

In a locked state the device is powered on but most of the functionality is unavailable for use. User authentication is required to access functionality. This functions as an access control but does not provide any DAR protection. The device is considered classified and should be handled accordingly.

6.2 PE/FE (PF) SOLUTION DESIGN

The PF Solution Design approach permits file/directory/volume encryption/decryption. In the PF solution design, DAR provided by the PE will be used as the outer layer and FE provided by an application will be used as the inner layer. The PF solution design relies on the EUD to implement the objective requirements in the Mobile Device Fundamentals (MDF) Protection Profile (PP). These objective requirements provide hardware-based protections for stored keys and ensuring adequate entropy collection.

The PE on a mobile EUD employs storage protection and entropy generation differently than on a fixed EUD (i.e. desktop, workstation, laptop, or server). Longer complex passwords can be levied against fixed EUD users more readily than against mobile EUD. Therefore, ensuring appropriate hardware-based protection for stored secrets and ensuring entropy is collected from hardware sensors in the mobile EUD for the PE layer of DAR protection is critical in reducing risk associated with storage of classified information. Integrators should note the FE does not meet this requirement, and will therefore require longer complex passwords for mobile EUDs. The PF solution is depicted below in Figure 5: PF Solution Design

Two other potential design considerations to be addressed by the customer/integrator include:

1.) A FE solution may be provided by the platform if and only if appropriate cryptographic separation and independence can be ensured in accordance with CSfC principles. This has the advantage of imposing no additional authentication requirements or restrictions on individual applications whatsoever. Most currently available FE solutions are implemented on a per application basis. This approach has a negative impact on user experience since the user must independently authenticate to each application providing FE solutions. In addition, it requires each application be evaluated against the FE PP, which creates a significant hurdle to expanding the number of applications available to the user.

2.) An application container may be used to protect the data from multiple applications. This would reduce the number of applications that must be evaluated against the FE PP at the expense of ensuring integration of each client application with the container. In each case, the cryptographic operations provided by either platform, container, or application shall be evaluated against FIPS 140-2 as part of the National Information Assurance Partnership (NIAP) test and evaluation process.

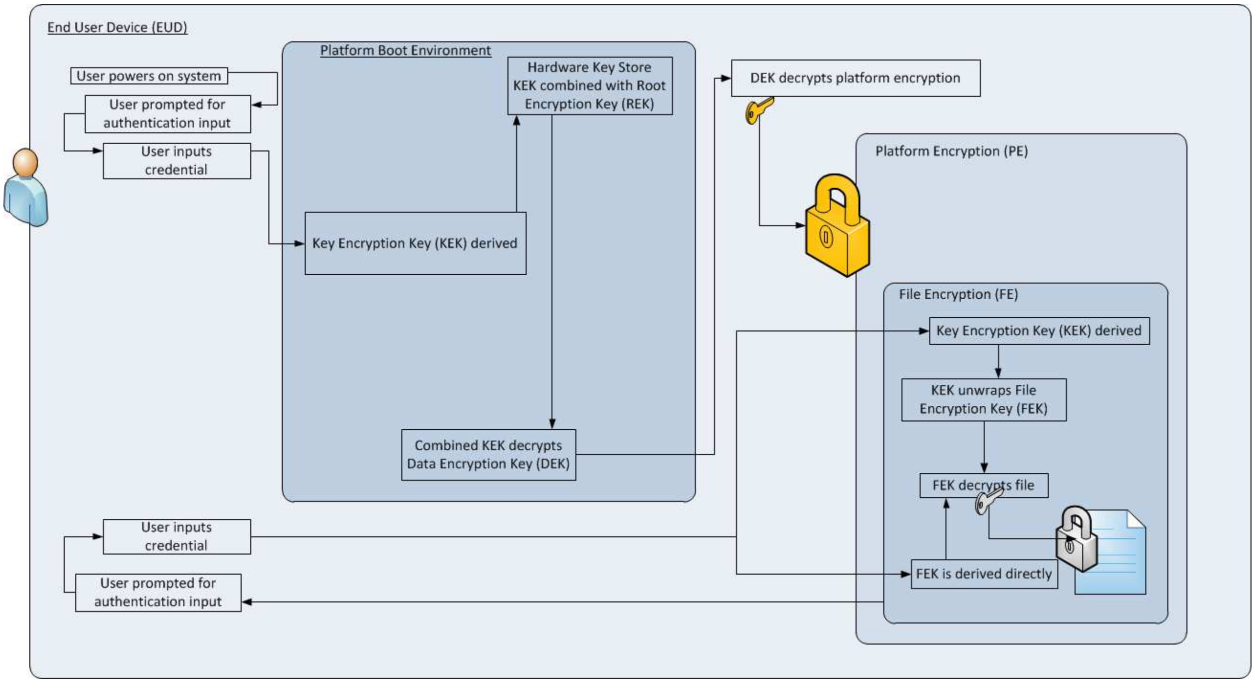
End User Device (EUD)
User powers on system
User prompted for authentication input
User inputs credential
Platform Boot Environment
Hardware Key Store KEK combined with Root Encryption Key (REK)
Key Encryption Key (KEK) derived
Combined KEK decrypts Data Encryption Key (DEK)
DEK decrypts platform encryption
Platform Encryption (PE)
File Encryption (FE)
Key Encryption Key (KEK) derived
KEK unwraps File Encryption Key (FEK)
FEK decrypts file
FEK is derived directly
User inputs credential
User prompted for authentication input

Figure 5: PF Solution Design

6.2.1 PF SOLUTION STATES

Powered Off State:

In a powered off state, the device is completely off and not in any power saving state. The EUD is considered Unclassified but must still be handled in accordance with the implementing organizations AO/DAA policies.

Powered On and Unauthenticated State:

In a powered on and unauthenticated state, the EUD is completely on, but the user has not logged in to either layer. The EUD is considered Unclassified, but must be handled in accordance with the implementing organization's AO/DAA policies.

Powered On with Outer Layer Authenticated State:

In a powered on state with outer layer authenticated, the device is operational where the user has authenticated to the outer layer of encryption. The device is considered classified and should be handled accordingly.

Powered On with Outer and Inner Layer Authenticated State:

In a powered on state with outer and inner layers authenticated, the EUD is operational, where the user has authenticated to two layers of DAR encryption. The device is considered classified and should be handled accordingly.

Locked State:

In a locked state, the device is powered on but most of the functionality is unavailable for use. User authentication is required to access functionality. This functions as an access control and may provide one layer of DAR protection. The device is considered classified and should be handled accordingly.

7. THREATS

This section details how the required components work together to provide overall security in the solution. Figures 4 and 5 show the boundary of the DAR solution covered by this CP. An assessment of security was conducted on the architecture described in this CP while making no assumptions regarding use of specific products for any of the defined components. There are several different threats to consider when evaluating the risk of protecting data-at-rest. By examining these threats the organization will have a better understanding of the risk they are accepting and how these risks affect the Confidentiality, Integrity, and Availability of the data.

7.1 PASSIVE THREATS

This threat refers to internal or external actors attempting to gain information from the EUD without changing the state of the system.

The security against passive attack targeting the DAR on the EUD is provided by the layered encryption layers. To mitigate passive attacks, two layers of Suite B encryption are employed to provide confidentiality for the solution. Use of Advanced Encryption Standard (AES) is approved to protect classified information, meeting IAD and CNSSP-15 guidance for adequate confidentiality. The DAR components used to set up the layers of encryption must be independent in a number of ways (see Section 8). Due to this independence, the adversary should not be able to exploit a single cryptographic implementation to compromise both layers of encryption.

7.2 EXTERNAL (ACTIVE) THREATS

This threat refers to outsiders gaining unauthorized access to classified Red data on the EUD. Threat actions include brute force attacks, or introduction of malware with the intention to compromise the EUD and gain access to Red data. Adversaries could gain access to the EUD and then exploit other devices once the EUD is connected to a network.

One method for preventing unauthorized access from an external attack is a reasonable password policy. It is required that each encryption layer have a form of user authentication. This will ensure that the data residing on the EUD will still be protected with at least one layer of encryption if the adversary is able to access one of the layers in the solution.

7.2.1 MALWARE AND UNTRUSTED UPDATES

Each DAR component of this solution has the option to receive updates only through direct physical administration or an NSA approved Data in Transit (DIT) solution (i.e. Type 1 or CSfC). This mitigates the threats of malicious users trying to push updates or code patches that can affect the security of the components. The source of all updates and patches should be verified before installation occurs.

7.2.2 SOCIAL ENGINEERING

It is the responsibility of the customer to define the appropriate policies and training necessary to protect against Social Engineering attacks. In addition, these types of attacks generally take advantage of other attacks detailed in Section 7.

7.3 INSIDER THREATS

This threat refers to an unauthorized or cleared person or group of people with access, physical or logical, to the EUD who may act maliciously or negligently, resulting in risk exposure for the organization. This threat could include poorly trained employees, curious employees, disgruntled employees, escorted personnel who gain access to the device, dishonest employees, or those that have the means and desire to gain access to the data residing on the EUD.

Threat actions include insertion or omission of data entries that result in loss of data integrity, willingly changing the configuration of an EUD, unwillingly or unknowingly executing a virus or malware, intentionally exposing the device to a virus or malware, cross-contaminating a EUD with data from a higher classification to a lower classification (e.g., Secret data to Unclassified device). Typically, the threat from insiders has the potential to cause the greatest harm to an organization, and insider attacks are also the hardest to monitor and track.

To mitigate insider threats, separation of roles within the solution is required (see Section 12). In addition it is recommended that each user of the solution have a unique user account (see Section 10.1).

7.4 SUPPLY CHAIN THREATS

A critical aspect of the U.S. Government's effectiveness is the dependability, trustworthiness, and availability of the Information and Communication Technology (ICT) components embedded in the systems upon which the ability to perform their mission rely. The supply chain for those ICT components are the underpinnings of those systems and networks and supply chain attacks are attempts to proactively compromise those underpinnings.

Unfortunately, the supplier cannot always provide guarantees of a safe delivery of a component. They are only able to provide assurances based on their reliance of established procedures and processes they have developed. In a single change of hands, the component may be introduced to potential threats and compromises on many levels.

The supply chain threat refers to an adversary gaining access to a vendor or retailer and then attempting to insert or install a modification or a counterfeit piece of hardware into a component destined for a U.S. Government customer in an effort to gain information or cause operational issues. This threat also includes the installation of malicious software on components of the solution. This threat is difficult to identify and test, and is increasingly more difficult to prevent or protect against since vendors build products containing components manufactured by subcontractors. It is often difficult to determine the source of where different pieces of components are built and installed within the supply chain.

Threat actions include manufacturing faulty or counterfeit parts of components that can be used to disrupt system or network performance, leaving open back doors in hardware that allow attackers easy ways to attack and evade monitoring, as well as easy ways to steal data or tamper with the integrity of existing/new data. Supply Chain attacks may occur during development and production, updates, distribution, shipping, at a warehouse, in storage, during operations, or disposal. For this reason, it is imperative that all components selected for use in CSfC solutions are subject to the applicable Supply Chain Risk Management (SCRM) process to reduce the risk of acquiring compromised components.

Each component that is selected from the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO/DAA-approved Product Supply Chain Threat Assessment process (See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance).

There are doctrinal requirements placed on Product Selection, Implementers, and System Integrators of these solutions to minimize the threat of supply chain attacks (see Sections 8, 10, and 11).

7.5 INTEGRATOR THREATS

This threat refers to an integrator who has unrestricted access to all components within the solution prior to the customer purchasing and implementing the solution within their system. This is different than a Supply Chain threat in that these integrators have access to all components to be used in the solution, rather than only those being procured from a particular vendor.

Threat actions could include installing or configuring components in a manner that places the organization at risk for attack or open to an unknown vulnerability that may not be detected through normal tests, scans, and security counter-measures. In order to mitigate this threat, integrators are required to be cleared to the highest level of data protected by the DAR solution. To further reduce the integrator threat, a customer may wish to use multiple integrators, such that no one integrator has access to all components of the solution.

8. DAR CONFIGURATION REQUIREMENTS

The following six sections (Sections 8 through 13) specify requirements for implementations of the SF and PF solution compliant with this CP. The tables of requirements in the following sections specify which of the following solution designs each requirement is applicable to:

- SF design: DAR solution components include SWFDE and FE.
- PF design: DAR solution components include PE and FE.

The CP includes two categories of requirements specified based on the guidance provide below:

- An Objective (O) requirement specifies a feature or function that is desired or expected. Organizations should implement objective requirements in lieu of the corresponding Threshold requirement where feasible.

- A Threshold (T) requirement specifies a minimum acceptable feature or function that still provides the needed capabilities if the corresponding objective requirement cannot reasonably be met (e.g., due to system maturity). A solution implementation must satisfy all applicable Threshold requirements, or their corresponding Objective requirements, in order to comply with this CP.

In many cases, the Threshold requirement also serves as the Objective requirement (T=O). In some cases, multiple versions of a requirement may exist in this Capability Package. Such alternative versions of a requirement are designated as being either a Threshold requirement or an Objective requirement. Where both a Threshold requirement and a related Objective requirement exist, the Objective requirement improves upon the Threshold requirement and may replace the Threshold requirement in future versions of this CP.

In order to comply with this CP, a solution must at minimum implement all Threshold requirements associated with each of the solution designs it supports, and should implement the Objective requirements associated with those solution designs where feasible. For example, a DAR solution utilizing a SWFDE and FE must implement the Threshold requirements only applicable to the SF design.

8.1 REQUIREMENTS DESIGNATORS

Each requirement defined in this CP has a unique identifier digraph that groups related requirements together (e.g. KM), and a sequence number (e.g. 2). The following table lists the digraphs used to group together related requirements, and identifies where they can be found in the following sections.

Table 3: Requirement Digraphs

Digraph	Description	Sections	Tables
PS	Product Selection Requirements	Section 9	Table 4
SR	Overall Solution Requirements	Section 10.1	Table 5
CR	Configuration Requirements for All DAR Components	Section 10.2	Table 6
SW	Requirements for SWFDE Components	Section 10.3	Table 7
PE	Requirements for PE Components	Section 10.4	Table 8
FE	Requirements for FE Components	Section 10.5	Table 9
EU	Requirements for EUD	Section 10.6	Table 10

Digraph	Description	Sections	Tables
CM	Configuration Change Detection Requirements	Section 10.7	Table 11
DM	Requirements for Device Management	Section 10.8	Table 12
AU	Auditing Requirements	Section 10.9	Table 13
KM	Key Management Requirements for All DAR Components	Section 10.10	Table 14
GD	Requirements for Use and Handling of Solutions	Section 11.1	Table 15
RP	Requirements for Incident Reporting	Section 11.2	Table 16
TR	Testing Requirements	Section 13	Table 17

9. REQUIREMENTS FOR SELECTING COMPONENTS

In this section, a series of requirements are given for maximizing the independence between the components within the solution. This will increase the level of effort required to compromise this solution.

Table 4: Product Selection Requirements

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-PS-1	The products used for the FE layer shall be chosen from the list of FE products on the CSfC Components List.	SF, PF	T=O	
DAR-PS-2	The products used for the SWFDE layer shall be chosen from the list of FDEs on the CSfC Components List.	SF	T=O	
DAR-PS-3	The products used for the PE layer shall be chosen from the list of Mobile Platform products on the CSfC Component List.	PF	T=O	

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-PS-4	The Inner and Outer DAR layer shall either: • come from different manufacturers, where neither manufacturer is a subsidiary of the other; or • be different products from the same manufacturer, where NSA has determined that the products meet the CSfC Program's criteria for implementation independence.	SF, PF	T=O	
DAR-PS-5	Each component selected from the CSfC Components List shall go through a Product Supply Chain Threat Assessment to determine the appropriate mitigations for the intended application of the component per the organization's AO/DAA approved Product Supply Chain Threat Assessment process. (See CNSSD 505 Supply Chain Risk Management (SCRM) for additional guidance.)	SF, PF	T=O	

10. CONFIGURATION

Once the products for the solution are selected, the next step is setting up the components and configuring them in a secure manner. This section consists of generic guidance for how to configure the components for a DAR solution.

10.1 OVERALL OPERATIONAL REQUIREMENTS

Table 5: Overall Solution Requirements

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-SR-1	Default accounts, passwords, community strings, and other default access control mechanisms for all components shall be changed or removed.	SF, PF	T=O	

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-SR-2	The DAR solution shall be properly configured according to local policy and U.S. Government guidance (e.g., DISA gold disk, NSA guidelines). In the event of conflict between the requirements in this CP and local policy, this CP takes precedence.	SF, PF	T=O	
DAR-SR-3	Each DAR EUD shall have unique user accounts.	SF, PF	O	optional

10.2 CONFIGURATION REQUIREMENTS FOR ALL DAR COMPONENTS

Table 6: Configuration Requirements for All DAR Components

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-CR-1	Default encryption keys shall be changed.	SF, PF	T=O	
DAR-CR-2	User authentication credential values for each DAR layer mechanism type shall be unique.	SF, PF	T=O	
DAR-CR-3	DAR components shall use algorithms for encryption selected from Table 1: Approved Suite B DAR Algorithms that are approved to protect the highest classification level of the data.	SF, PF	T=O	
DAR-CR-4	Each DAR component shall prevent further authentication attempts after no more than 5 consecutive failed logon attempts as defined by the AO/DAA.	SF, PF	O	optional
DAR-CR-5	Each DAR layer shall zeroize the Data Encryption Key after a number consecutive failed logon attempts as defined by the AO/DAA.	SF, PF	O	optional
DAR-CR-6	Each DAR component shall generate its own symmetric encryption keys.	SF, PF	T=O	
DAR-CR-7	Each DAR component shall be configured to enable only an	SF, PF	T=O	

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
	administrator to disable DAR component.			
DAR-CR-8	All components shall have DAR protections enabled at all times after provisioning.	SF, PF	T=O	
DAR-CR-9	All components shall encrypt all classified data.	SF, PF	T=O	
DAR-CR-10	All CSfC components shall be implemented (configured) using only their NIAP-approved configuration settings.	SF, PF	T=O	

10.3 REQUIREMENTS FOR SWFDE COMPONENTS

Table 7: Requirements for SWFDE Components

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-SW-1	The SWFDE shall use Cipher Block Chaining (CBC) or Exclusive or (Xor)-encrypt-xor (XEX)-based tweaked-codebook mode with ciphertext stealing (XTS) for encryption.	SF	T=O	
DAR-SW-2	The SWFDE shall be configured to use one of the following authentication options: • A passphrase or password with the length and complexity defined by the AO/DAA; or • A randomly-generated bit string contained on an external USB token; or • A combination of a passphrase and external token.	SF	T=O	

10.4 REQUIREMENTS FOR PE COMPONENTS

Table 8: Requirements for PE Components

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-PE-1	The PE shall enable the “wipe sensitive data” management function for imported or self-generated keys/secrets and/or other classified data.	PF	T=O	
DAR-PE-2	The PE shall use CBC, Galois/Counter Mode (GCM) or XTS for Encryption.	PF	T=O	
DAR-PE-3	The AO/DAA shall provide policy to the user determining when data or keys must be wiped.	PF	T=O	
DAR-PE-4	The PE shall use one of the following authentication options: • A pin, passphrase or password with the length and complexity defined by the AO/DAA	PF	T=O	

10.5 REQUIREMENTS FOR FE COMPONENTS

Table 9: Requirements for FE Components

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-FE-1	System folders shall have user write permissions disabled unless authorized by an administrator.	SF, PF	T=O	
DAR-FE-2	The FE shall use Cipher Block Chaining (CBC), Counter with CBC- Message Authentication Moded (MAC) (CCM) or XTS for Encryption.	SF, PF	T=O	
DAR-FE-3	The FE shall enable zeroization of all cryptographic keys per AO/DAA guidelines.	SF, PF	O	optional
DAR-FE-4	Users shall be restricted to designated user folders.	SF, PF	T=O	
DAR-FE-5	The FE shall encrypt all user folders.	SF, PF	T=O	

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-FE-6	The FE shall only allow administrators to disable data-at-rest protection.	PF	O	optional
DAR-FE-8	The FE shall use the Trust Anchor Database protected storage.	PF	O	optional
DAR-FE-9	The FE shall use one of the following authentication options: • A passphrase or password with the length and complexity defined by the AO/DAA; or • An external smartcard containing a software certificate with RSA or ECC key pairs; or • A software certificate protected by a password/passphrase	SF, PF	T=O	

10.6 REQUIREMENTS FOR END USER DEVICES

Table 10: Requirements for End User Devices

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-EU-1	All EUD provisioning shall be performed through direct physical access.	SF, PF	T=O	
DAR-EU-2	The EUDs shall be destroyed if found after being lost. (This does not preclude forensic investigation by appropriate authority.)	SF, PF	T=O	
DAR-EU-3	EUDs shall implement the BIOS security guidelines specified in NIST SP 800-147.	SF, PF	O	optional
DAR-EU-4	All Users shall sign an organization-defined user agreement before being authorized to use a EUD.	SF, PF	T=O	
DAR-EU-5	All Users shall receive an organization-developed training course for operating an EUD prior to use.	SF, PF	T=O	
DAR-EU-6	At a minimum, the organization defined user agreement shall	SF, PF	T=O	

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
	include each of the following: • Consent to monitoring • OPSEC guidance • Required physical protections to employ when operating and the EUD • Restrictions for when and where the EUD may be used • Verification of IA Training • Verification of appropriate clearance • Justification for Access • Requester information and organization • Account Expiration Date • User Responsibilities			
DAR-EU-7	USB tokens and Smartcards, when used, shall be removed from the EUD when shut down in accordance with AO/DAA policy.	SF	T=O	
DAR-EU-8	AO/DAA shall provide guidance on storing and securing authentication factors.	SF, PF	T=O	
DAR-EU-9	The security administrator shall disable system power states on EUDs (i.e. Sleep and Hibernate).	SF, PF	T=O	
DAR-EU-10	The EUD shall shut down after a period of inactivity defined by the AO/DAA, not to exceed 2 hours.	SF	T=O	
DAR-EU-11	The EUDs shall be provisioned within a physical environment certified to protect the highest classification level of the data stored on the device.	SF, PF	T=O	
DAR-EU-12	The EUD shall only be reprovisioned to the same classification level of the Red data from an approved DAR solution.	SF, PF	T=O	
DAR-EU-13	The EUD shall be reported as “lost” if out of an authorized user’s control for an AO defined time period not to exceed 20 minutes.	SF, PF	T=O	
DAR-EU-14	The EUD shall mark data as classified and keys as sensitive.	PF	T=O	

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-EU-15	The EUD shall transition to a locked state after a time interval of inactivity as defined by the AO/DAA, not to exceed 20 minutes.	SF, PF	T=O	
DAR-EU-16	The EUD shall transition to a locked state after a user-initiated lock command.	SF, PF	T=O	
DAR-EU-17	The EUD shall import keys from the FE into the secure key storage.	PF	T=O	

10.7 CONFIGURATION CHANGE DETECTION REQUIREMENT

Table 11: Configuration Change Detection Requirements

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-CM-1	A baseline configuration for all components shall be maintained by the System Administrator and be available to the Auditor.	SF, PF	T=O	
DAR-CM-2	An automated process shall ensure that configuration changes are logged.	SF, PF	O	optional
DAR-CM-3	Log messages generated for configuration changes shall include the specific changes made to the configuration.	SF, PF	O	optional

10.8 REQUIREMENTS FOR DEVICE MANAGEMENT

Only authorized Security Administrators (See Section 12) will be allowed to administer the DAR Components.

Remote administration for software updates and re-configuration can be utilized through an approved NSA DIT solution.

If the solution owner is unable to remotely manage the EUDs, the solution owner must physically manage all devices in order to ensure the device(s) and DAR protection components receive the proper software and configuration updates.

Table 12: Requirements for Device Mangament

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-DM-1	EUDs shall be physically administered.	SF, PF	T	
DAR-DM-2	EUDs shall be remotely administered using a NSA approved DIT protection solution (e.g. NSA Certified or CSfC approved).	SF, PF	O	DAR-DM-1

10.9 AUDITING REQUIREMENTS

Table 13: Auditing Requirements

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-AU-1	EUDs shall be inspected for malicious physical changes in accordance with AO/DAA defined policy.	SF, PF	T=O	
DAR-AU-2	The EUDs shall be configured to generate an audit record of the following events: • Start-up and shutdown of any platform audit functions. • All administrative actions affecting the DAR encryption components. • User authorization attempts and success/failure of the attempts. • Software updates to the DAR encryption components.	SF, PF	O	optional
DAR-AU-3	Auditors shall review audit logs for an AO/DAA defined time period not to exceed 3 months.	SF,PF	T=O	
DAR-AU-4	Auditors shall physically account for the EUDs after an AO/DAA defined time period not to exceed 3 months.	SF, PF	T=O	
DAR-AU-5	Administrators shall periodically compare solution component configurations to a trusted baseline configuration after an AO/DAA defined time period not to exceed 3 months.	SF, PF	O	optional

10.10 KEY MANAGEMENT REQUIREMENTS

Table 14: Key Management Requirements for All DAR Components

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-KM-1	The KEK, FEK, and DEK key sizes and algorithms used for the SW FDE and FE shall be as specified in Table 1.	SF, PF	T=O	
DAR-KM-2	DAR solution products shall be initially keyed within a physical environment certified to protect the highest classification level of the DAR solution.	SF, PF	T=O	
DAR-KM-3	The DAR solution shall disable all key recovery mechanisms.	SF, PF	T=O	

11. REQUIREMENTS SOLUTION OPERATION, MAINTENANCE, AND HANDLING

11.1 REQUIREMENTS FOR THE USE AND HANDLING SOLUTIONS

The following requirements shall be followed regarding the use and handling of the solution.

Table 15: Requirements for Use and Handling of Solutions

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-GD-1	Acquisition and procurement documentation shall not include information about how the equipment will be used, including that it will be used to protect classified information.	SF, PF	T=O	
DAR-GD-2	The solution owner shall allow, and fully cooperate with, NSA or its authorized agent to perform an IA compliance audit (including, but not limited to, inspection, testing, observation, interviewing) of the solution implementation to ensure it meets the latest version of the Capability Package.	SF, PF	T=O	
DAR-GD-3	The AO/DAA will ensure that a compliance audit shall be conducted every year against the latest version of the DAR Capability Package.	SF, PF	T=O	

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-GD-4	Results of the compliance audit shall be provided to and reviewed by the AO/DAA.	SF, PF	T=O	
DAR-GD-5	When a new approved version of the DAR Capability Package is published by NSA, the AO/DAA shall ensure compliance against this new Capability Package within 6 months.	SF, PF	T=O	
DAR-GD-6	Solution implementation information, which was provided to NSA during solution registration, shall be updated every 12 (or less) months (see Section 13.3).	SF, PF	T=O	
DAR-GD-7	The Security Administrator, Auditor, User, and all Solution Integrators shall be cleared to the highest level of data protected by the DAR solution.	SF, PF	T=O	
DAR-GD-8	The Security Administrator and Auditor roles shall be performed by different people.	SF, PF	T=O	
DAR-GD-9	All Security Administrators, Users, and Auditors shall meet local information assurance training requirements.	SF, PF	T=O	
DAR-GD-10	User shall report lost or stolen EUDs to their Information System Security Officer (ISSO) (i.e., chain of command) as defined by the AO/DAA.	SF, PF	T=O	
DAR-GD-11	Only Security administrators shall perform the installation and policy configuration.	SF, PF	T=O	
DAR-GD-12	Security critical patches (such as IAVAs) shall be tested and subsequently applied to all components in the solution in accordance with local policy and this Capability Package.	SF, PF	T=O	
DAR-GD-13	Local policy shall dictate how the System Administrator will install patches to solution components.	SF, PF	T=O	
DAR-GD-14	All authorized Users shall have the ability to zeroize keys for both layers.	SF, PF	O	optional

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-GD-15	When using an FE Product, user must ensure that no classified data shall be put in the file metadata (e.g., filename)	SF, PF	T=O	
DAR-GD-16	All components in the solution shall be disposed of as classified devices, unless declassified using AO/DAA-approved procedures.	SF, PF	T=O	

11.2 Requirements for Incident Reporting

Table 16 lists requirements for reporting security incidents to NSA, to be followed in the event a solution owner identifies a security incident which affects the solution. These reporting requirements are intended to augment, not replace, any incident reporting procedures already in use within the solution owner's organization. It is critical that Security Administrators (SAs) and Auditors are familiar with maintaining the solution in accordance with this CP. Based on familiarity with the known-good configuration of the solution, personnel responsible for Operations and Maintenance (O&M) will be better equipped to identify reportable incidents.

A security failure, in this context, includes reporting any malfunction in any of the DAR components due to faulty code, operator error, or specification error.

For the purposes of incident reporting, "malicious" activity includes not only events that have been attributed to activity by an adversary but also any events that are unexplained. In other words, an activity is assumed to be malicious unless it has been determined to be the result of known non-malicious activity.

Compromise, in this context, includes reporting real or perceived access to classified data (for e.g. user or administrator access or permission to data without having to authenticate or using incorrect credentials) .

Table 16 only provides requirements directly related to the incident reporting process. See Section 10.9 for requirements supporting detection of events that may reveal that a reportable incident has occurred.

Table 16. Incident Reporting Requirements

Req #	Requirement Description	Solution designs	Threshold / Objective	Alternative
DAR-RP-1	Report a security failure in any of the CSfC DAR solution components.	SF, PF	T	
DAR-RP-2	Report any malicious configuration changes to the DAR components	SF, PF	T	
DAR-RP-3	Report any evidence of a compromise of classified data caused by a failure of the CSfC DAR solution.	SF, PF	T	
DAR-RP-4	Report any evidence of malicious physical tampering(i.e., missing or mis-installed parts) with solution components.	SF, PF	T	
DAR-RP-5	Confirmed incidents meeting the criteria in DAR-RP-1 thru DAR-RP-4 shall be reported via Joint Incident Management System (JIMS) or contacting the NSA as specified in the CSfC Registration Letter within at time defined by AO/DAA.	SF, PF	T	
DAR-RP-6	At a minimum, the organization shall provide the following information when reporting security incidents: • CSfC Registration Number • Point of Contact (POC) name, phone, email • Alternate POC name, phone, email • Classification level of affected solution • Affected component(s) manufacturer/vendor • Affected component(s) model number • Affected component(s) version number • Date and time of incident • Description of incident • Description of remediation activities • Is Technical Support from NSA requested? (Yes/No)	SF, PF	T	

12. ROLE-BASED PERSONNEL REQUIREMENTS

The roles required to administer and maintain the solution are detailed below, along with doctrinal requirements for these roles.

End User – An End User may operate a EUD from physical locations not owned, operated, or controlled by the government. The End User shall be responsible for operating the EUD in accordance with this CP and an organization defined user agreement. End User duties include, but are not limited to:

1) Ensuring the EUD is only operated in physical spaces which comply with the end user agreement.
2) Alerting the Security Administrator immediately upon a EUD being lost, stolen, or suspected of being tampered with.

Security Administrator – The Security Administrator shall be responsible for maintaining monitoring, and controlling all security functions for the entire suite of products composing the DAR solution. Security Administrator duties include but are not limited to:

1) Ensuring that the latest security critical software patches and updates (such as IAVAs) are applied to each product in a timely fashion.
2) Documenting and reporting security-related incidents to the appropriate authorities.
3) Coordinating and supporting product logistic support activities including integration and maintenance. Some logistic supports activities may require that the Security Administrator escort uncleared personnel.
4) Ensuring that the implemented DAR solution remains compliant with the latest version of the CP.
5) Provisioning and maintaining EUDs in accordance with this CP.

Auditor – The Auditor shall be responsible for reviewing the actions performed by the Security Administrator and events recorded in the audit logs to ensure that no action or event represents a compromise of the DAR solution. The role of Auditor and Security Administrator shall not be performed by the same individual. Auditor duties include but are not limited to:

1) Reviewing, managing, controlling, and maintaining security audit log data
2) Documenting and reporting security related incidents to the appropriate authorities.
3) The Auditor will only be given authority to access all audit record.

Solution Integrator – In certain cases, an external integrator may be hired to implement a DAR solution based on the CP. Solution Integrator duties may include but are not limited to:

1) Acquiring the products that compose the solution.
2) Configuring the DAR solution in accordance with the CP.
3) Testing the DAR solution.
4) Documenting the solution.
5) Troubleshooting the solution.

13. INFORMATION TO SUPPORT AO/DAA

This section details items that likely will be necessary for the customer to obtain approval from the system AO/DAA. The customer and AO/DAA have obligations to perform the following:

- The customer, possibly with support from a System Integrator, instantiates a solution implementation that follows the NSA-approved CP.
- The customer has a testing team develop a Test Plan and perform testing of the DAR solution, see Section 13.1.
- The customer has system certification and accreditation performed using the risk assessment information referenced in Section 13.2.
- The customer provides the results from testing and system certification and accreditation to the AO/DAA for use in making an approval decision. The AO/DAA is ultimately responsible for ensuring that all requirements from the CP have been properly implemented.
- The customer registers the solution with NSA and re-registers yearly to validate its continued use as detailed in Section 13.3.
- Customers who want to use a variant of the solution detailed in this CP will contact NSA early in their design phase to determine ways to obtain NSA approval.
- The AO/DAA will ensure that a compliance audit shall be conducted every year against the latest version of the DAR CP, and the results shall be provided to the AO/DAA.

13.1 SOLUTION TESTING

This section provides a framework for a Test and Evaluation (T&E) plan and procedures to validate the implementation of a DAR solution. This T&E will be a critical part of the approval process for the AO/DAA, providing a robust body of evidence that shows compliance with this CP.

The security features and operational capabilities associated with the use of the solution shall be tested. The following is a general high-level methodology for developing the test plan and procedures and for the execution of those procedures to validate the implementation and functionality of the DAR solution. The entire solution, to include each component described in Section 5, is addressed by this test plan.

1) Set up the baseline network architecture and configure all components.
2) Document the baseline network architecture configuration. Include product model and serial numbers, and software version numbers as a minimum.
3) Develop a test plan for the specific implementation using the test objectives from Section 14. Any additional requirements imposed by the local AO/DAA should also be tested, and the test plan shall include tests to ensure that these requirements do not interfere with the security of this solution as described in this CP.

4) Perform testing using the test plan derived in Step 3. System testing will consist of both Black Box testing and Gray Box testing. A two-person testing approach should be used to administer the tests. During test execution, security and non-security related discrepancies with the solution shall be documented.
5) Compile findings, to include comments and vulnerability details as well as possible countermeasure information, into a final test report to be delivered to the AO/DAA for approval of the solution.
6) The following testing requirement has been developed to ensure that the DAR solution functions properly and meets the configuration requirements from Section 8. Testing of these requirements should be used as a minimum framework for the development of the detailed test plan and procedures.

Table 17: Test Requirements

Req #	Requirement Description	Solution designs	Threshold / Objective
DAR-TR-1	The organization implementing the CP shall perform all test listed in Section 14.	SF, PF	T=O

13.2 Risk Assessment

The risk assessment (RA) of the DAR solution presented in this CP focuses on the types of attacks that are feasible against this solution and the mitigations that can be employed. Customers should contact their NSA/IAD Client Advocate to request the risk assessmnet, or visit the Secret Internet Protocol Router Network (SIPRNet) CSfC site for information. The process for obtaining the RA is available on the SIPRNet CSfC website. The AO/DAA shall be provided a copy of the NSA RA for their consideration in approving the use of the solution.

13.3 Registration of Solutions

All customers using CSfC solutions to protect information on National Security Systems shall register their solution with NSA prior to operational use. Customers will provide their compliance checklists and registration forms to NSA. This registration will allow NSA to track where DAR CP solutions are instantiated and to provide AO/DAAs at those sites with appropriate information, including any significant vulnerabilities that may be discovered in components or high-level designs approved for these solutions. The CSfC solution registration process, as well as the compliance matrices and registration forms, are available at http://www.nsa.gov/ia/programs/csfc_program.

Solution registrations are valid for one year, at which time customers are required to re-register their solution in order to continue using it. Approved CPs will be reviewed twice a year, or as events warrant. Registered users of this CP will be notified when an updated version is published. When a new version of this CP that has been approved by the IAD Director is published, customers will have six months to bring their solutions in compliance with the new version and re-register their solution (see requirement DAR-GD-5). Customers are also required to update their registrations whenever the information provided on the registration form changes.

14. TESTING REQUIREMENTS

This section contains the specific tests that allow the Security Administrator or System Integrator to ensure they have properly configured the solution. As defined in Section 8, in order to comply with this CP, a solution must at minimum implement all Threshold requirements associated with each of the capabilities it supports, and should implement the Objective requirements associated with those capabilities where feasible. These tests may also be used to provide evidence to the AO/DAA regarding compliance of the solution with this CP. Note that the details of the procedures are the responsibility of the final developer of the test plan in accordance with AO/DAA-approved network procedures. The AO/DAA is ultimately responsible for ensuring that all requirements from the CP have been properly implemented.

APPENDIX A. GLOSSARY OF TERMS

Accreditation – The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37)

Assurance – A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy.

Audit – The activity of monitoring the operation of a product from within the product. It includes monitoring of a product for a set of pre-determined events. Each audit event may indicate rogue behavior, or a condition that is detrimental to security, or provide necessary forensics to identify the source of rouge behavior.

Capability Package (CP) – The set of guidance provided by NSA that describes recommended approaches to composing COTS components to protect classified information for a particular class of security problem. This package will point to potential products that can be used as part of this solution.

Certification – The technical evaluation of a systems’ security features, made as part of and in support of the approval/accreditation process that establishes the extent to which a particular computer systems design and implementation meet a set of specified security requirements.

Certification and Accreditation (C&A) – A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. In conjunction with the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. (NIST 800-37).

Committee on National Security Systems Policy No. 15 (CNSSP-15) – Policy specifies which public standards may be used for cryptographic protocol and algorithm interoperability to protect National Security Systems (NSS).

Designated Approving Authority (DAA) – The official with the authority to formally assume responsibility for opening a system at an acceptable level of risk, synonymous with designating accrediting authority and delegated accrediting authority. [CNSSI 4009]

End User Device (EUD) – A device such as a workstation, laptop, tablet, or cellular phone that serves as the platform and host through which the user stores classified data to the DAR solution.

Federal Information Processing Standards (FIPS) – A set of standards that describe the handling and processing of information within governmental agencies.

File Encryption (FE) – The process of encrypting individual files, folders or volumes, and permitting access to the data only after successful authentication with the file encryption product.

Found Device - A lost device that has been recovered. (see Lost Device definition)

Full Disk Encryption (FDE) – The process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication within the Pre-Boot Environment (see Pre-Boot Environment definition)..

Lost Device - A device that is removed from the control of the physical security procedures defined by the AO/DAA.

Platform Encryption (PE) – the process of encrypting all of the data on a volume and permitting access to the data only after successful authentication with encryption software. PE is implemented natively by the EUD's platform. (see Volume definition)

Pre-Boot Environment (PBE) – The inital software run on start-up of the EUD which requires a user to authenticate successfully before decrypting and booting an operating system. This is the layer of authentication for the FDE product.

Protection Profile (PP) – A document used as part of the certification process according to the Common Criteria. As the generic form of a security target, it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.

Supply Chain Risk Management (SCRM) —A program to establish processes and procedures to minimize acquisition-related risks to critical acquisitions including, hardware components and software solutions from supply chain threats due to reliance on global sources of supply.

Trusted Platform Module (TPM) Chip – A tamper-resistant integrated circuit built into some computer motherboards that can perform cryptographic operations (including key generation) and protect small amounts of classified data, such as passwords and cryptographic keys.

Volume - a collection of separate units of logically divided media (partition) acting as a single entity that has been formatted with a file system.

APPENDIX B. ACRONYMS

AES	Advanced Encryption Standard
AO	Authorizing Official
BIOS	Basic Input/Output System
C&A	Certification and Accreditation
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CNSSP	Committee on National Security Systems Policy
COTS	Commercial Off-the-Shelf
CP	Capability Package
CSfC	Commercial Solutions for Classified
DAA	Designated Approving Authority
DAR	Data-at-Rest
DEK	Data Encryption Key
DH	Diffie Hellman
DIT	Data in Transit
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EUD	End User Device
FE	File Encryption
FEK	File Encryption Key
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standards
GCM	Galois/Counter Mode
IAD	Information Assurance Directorate
IAVA	Information Assurance Vulnerability Alert
ICT	Information and Communication Technology
ISSO	Information System Security Officer
ISV	Independent Software Vendor
JIMS	Joint Incident Management System
KEK	Key Encryption Key
MAC	Message Authentication Code
MDF	Mobile Device Fundamentals

NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
OS	Operating System
PBE	Pre-Boot Environment
PE	Platform Encryption
POC	Point of Contact
PP	Protection Profile
REK	Root Encryption Key
RFC	Request for Comment
RSA	Rivest Shamir Adelman algorithm
S3	Secure Sharing Suite
SCRM	Supply Chain Risk Management
SHA	Secure Hash Algorithm
SIPRNet	Secret Internet Protocol Router Network
SW	Software
T&E	Test and Evaluation
TPM	Trusted Platform Module
USB	Universal Serial Bus
XES	Exclusive or (Xor)-encrypt-xor
XTS	XEX-based tweaked-codebook mode with ciphertext stealing

APPENDIX C. REFERENCES

CNSSI 4009	*CNSSI 4009, National Information Assurance (IA) Glossary Committee for National Security Systems www.cnss.gov/Assets/pdf/cnssi_4009.pdf*	April 2010
CNSSP 15	*CNSS Policy (CNSSP) Number 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems Committee for National Security Systems*	March 2010
CNSSD 505	*CNSS Directive (CNSSD) Number 505, Supply Chain Risk Management (SCRM)*	March 2012
CSfC	*CSfC Incident Reporting Procedures*	June 2014
FIPS 180	*Federal Information Processing Standard 180-4, Secure Hash Standard (SHS)*	March 2012
FIPS 186	*Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), (Revision of FIPS 186-2, June 2000)*	June 2009
FIPS 197	*Federal Information Processing Standard 197, Advanced Encryption Standard (AES)*	November 2001
FIPS 201	*Federal Information Processing Standard 201, Personal Identity Verification (PIV) of Federal Employees and Contractors National Institute for Standards and Technology FIPS Publication http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf*	March 2006
FE PP	*File Encryption Protection Profile. www.niap.ccevs.org/pp*	**[in draft, update]**
MDF PP	*Mobile Device Fundamentals Protection Profile. www.niap.ccevs.org/pp*	October 2013
NSA Suite B	*NSA Guidance on Suite B Cryptography [including the Secure Sharing Suite (S3)]. http://www.nsa.gov/ia/programs/ suiteb_cryptography/index.shtml*	November 2010
SW FDE PP	*Software Full Disk Encryption Protection Profile. www.niap.ccevs.org/pp*	February 2013
SP 800-56A	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. E. Barker, D. Johnson, and M. Smid*	March 2007

SP 800-56B	*NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography. E. Barker, et. al.*	August 2009
SP 800-56C	*NIST Special Publication 800-56C, Recommendation for Key Derivation through Extraction-then-Expansion. L. Chen.*	November 2011
SP 800-111	*NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices*	November 2007
SP 800-131A	*NIST Special Publication 800-131A, Recommendation for Transitioning of Cryptographic Algorithms and Key Lengths. E. Barker.*	January 2011
SP 800-132	*Recommendation for Password-Based Key Derivation*	December 2010
SP 800-147	*NIST Special Publication 800-147, BIOS Protection Guidelines. D. Cooper, et. al.*	April 2011